REMARKS/ARGUMENTS

In the Office Action, the Examiner noted that claims 1-22, 24-25, 27, 56-64, 66-76, and 79-83 are pending in the application. The Examiner additionally stated that claims 1-22, 24-25, 27, 56-64, 66-76, and 79-83 are rejected. By this communication, claims 1, 14-15, 56, and 68-69 are amended. Hence, claims 1-22, 24-25, 27, 56-64, 66-76, and 79-83 are pending in the application.

Applicant hereby requests further examination and reconsideration of the application, in view of the foregoing amendments.

In the Claims

Rejections Under 35 U.S.C. §103(a)

The Examiner rejected claims 1-6, 11-12, 24-25, 27, 56-60, 66, and 79-83 under 35 U.S.C. 103(a) as being unpatentable over Kessler et al., U.S. Patent 6,789,147 (hereinafter, Kessler) in view of Bakhle et al., U.S. Patent 6,021,201 (hereinafter, Bakhle), in view of Best, U.S. Patent 4,278,837, (hereinafter, Best), in view of "PC Hardware in a Nutshell" (hereinafter, Thomspson). Applicant respectfully traverses the Examiner's rejections.

Claim 1 recites:

1. A microprocessor apparatus, for performing a cryptographic operation, the apparatus comprising:

an x86-compatible microprocessor, comprising:

fetch logic, configured to fetch an application program from memory for execution by said x86-compatible microprocessor, said application program comprising:

an atomic instruction, configured to direct said x86-compatible microprocessor to perform the cryptographic operation, wherein said atomic instruction comprises:

an opcode field, configured to prescribe that said x86-compatible microprocessor accomplish the cryptographic operation as further specified within a control word stored in said memory; and

a repeat prefix field, coupled to said opcode field, configured to indicate that the cryptographic operation prescribed by the atomic instruction is to be accomplished on a plurality of blocks of input data;

a cryptography unit, configured to execute a plurality of cryptographic rounds on each of a plurality of input text blocks to generate a corresponding each of a plurality of output text blocks, wherein said plurality of cryptographic rounds are prescribed by said control word, wherein said cryptography unit executes a first plurality of micro instructions generated by translation of said cryptographic instruction; and

an x86 integer unit, an x86 floating point unit, an x86 MMX unit, and an x86 SSE unit, wherein said cryptography unit operates in parallel with said x86 integer unit, said x86 floating point unit, said x86 MMX unit, and said x86 SSE unit, to accomplish the cryptographic operation, wherein said x86 integer unit executes a second plurality of micro instructions generated by said translation unit to test a bit in a flags register, to update text pointer registers, and to process interrupts during execution of said plurality of cryptographic rounds.

Nowhere does the cited art disclose **wherein said x86 integer unit executes a second plurality of micro instructions generated by said translation unit to test a bit in a flags register, to update text pointer registers, and to process interrupts during execution of said plurality of cryptographic rounds**, as is recited in claim 1. The

Examiner incorrectly assumes that the limitation "wherein said cryptography unit operates in parallel with said x86 integer unit, said x86 floating point unit, said x86 MMX unit, and said x86 SSE unit, to accomplish the cryptographic operation" implies that these units do not participate in the processing of the atomic cryptographic instruction, and it is argued that the specification does not support the contention that parallel operation of these units is required. In response, Applicant has amended claim 1 to specifically recite a first plurality of micro instructions that are directed to the cryptography unit, and a second plurality, noted above, that are executed by the integer unit to perform other operations necessary to accomplish the cryptographic operation. Support for this limitation is found in several places in the specification. For example, see paragraph [0052].

Clearly, the cited art fails to disclose a x86-compatible microprocessor comprising the noted elements. Kessler utterly fails to teach any form of microprocessor whatsoever. Bakhle fails to teach any form of an x86-compatible microprocessor as is recited according to the above limitation. The microprocessor of Best (Fig. 17, 100) is void of any of the recited elements as well. Thompson indeed discloses an x86 integer unit, x86 floating point unit, x86 MMX unit, or x86 SSE unit. However, none of the cited references teach or suggest two pluralities of micro instructions executed in parallel by a cryptographic unit and an x86 integer unit in order to accomplish an atomic cryptographic operation.

Accordingly, since Applicant has shown that the cited art utterly fails to disclose the elements noted above, it is respectfully requested that the rejection of claim 1 be withdrawn.

Claim 56 recites substantially the same elements and limitations as are argued above as being allowable over the prior art of record, and consequently Applicant respectfully asserts that claim 56 is both novel and nonobvious as well, and it is thus requested that the rejection of this claim be withdrawn.

With respect to claims 2-6, 11-12, 24-25, 27, 56-60, 66, and 79-83, these claims depend from claims 1 and 56 as appropriate, and add further limitations that are neither

anticipated nor made obvious by the cited references. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 2-6, 11-12, 24-25, 27, 56-60, 66, and 79-83.

The Examiner rejected claims 7-10 and 61-64 under 35 U.S.C. 103(a) as being unpatentable over Kessler in view of Bakhle in view of Best in view of Thompson, as noted above, and further in view of "Applied Cryptography, 2nd Edition."

Applicant respectfully traverses the Examiner's rejections and notes that claims 7-10 and 61-64, depend from claims 1 and 56, respectively, and add further limitations over that subject matter which is argued above as being allowable over the prior art of record. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 7-10 and 61-64.

The Examiner additionally rejected claims 13-22 and 67-76 under 35 U.S.C. 103(a) as being unpatentable over Kessler in view of Bakhle in view of Best in view of Thompson, and further in view of Johns-Vano et al. (U.S. Patent 6,026,490). Applicant respectfully traverses and notes that claims 13-22 and 67-76 depend from claims 1 and 56, respectively, and add further limitations over that subject matter which is argued above as being allowable over the prior art of record. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 13-22 and 67-76.

CONCLUSIONS

Applicant believes this to be a complete response to all of the issues raised in the instant office action and further submits, in view of the amendments and arguments advanced above, that claims 1-22, 24-25, 27, 56-64, 66-76, and 79-83 are in condition for allowance. Reconsideration of the rejections is requested, and allowance of the claims is solicited.

Applicant also notes that any amendments made by way of this response, and the observations contained herein, are made solely for the purpose of expediting the patent application process in a manner consistent with the PTO's Patent business Goals (PBG), 65 Fed. Reg. 54603 (September 8, 2000), and are furthermore made without prejudice to Applicant under this or any other jurisdictions. It is moreover asserted that insofar as any subject matter might otherwise be regarded as having been abandoned or effectively disclaimed by virtue of amendments made herein and/or incorporated in attachments submitted with this response, Applicants wishes to reserve the right and hereby provides notice of intent to restore such subject matter and/or file a continuation application in respect thereof.

Applicant earnestly requests that the Examiner contact the undersigned practitioner by telephone if the Examiner has any questions or suggestions concerning this amendment, the application, or allowance of any claims thereof.

Respectfully submitted,
HUFFMAN PATENT GROUP, LLC

/Richard K. Huffman/

By: _____

RICHARD K. HUFFMAN, P.E.
Registration No. 41,082
Tel: (719) 575-9998

06/22/2010

Date: _____